CA™ SiteMinder® ERP Agents

Agent Guide for SAP ITS

r5.6 SP4

CA Product References

This document references the following CA products:

- CA™ SiteMinder®

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Contents

Chapter 4: Troubleshooting and Messages 29

Appendix A: NPSEncrypt and NPSVersion Tools 35

Index 39

Chapter 1: Overview and Architecture

This section contains the following topics:

Background

Internet Transaction Server

SAP provides a web-based interface to many SAP applications through a web server component known as Internet Transaction Server (ITS). ITS controls the data flow between, and is made up of a web server (web gateway, or WGate) and an application server (application gateway, or AGate), allowing users access to business applications that are enabled for the Web.

Single Signon Options

Typically, when a user attempts to execute an SAP transaction, SAP ITS prompts the user for username, password, and language via an HTML form. Once authenticated, SAP executes the requested transaction.

SAP has two techniques for supporting single signon (SSO):

- SSO Cookies—this option stores the user's username and password in an encrypted cookie. SAP recommends this option only for legacy application support.
- SSO2 Tickets—this option is more flexible than SSO Cookies and is the preferred mechanism for achieving single signon. The SSO2 Ticket is also stored in a cookie, however, instead of storing a username and password, the user's identity, session start time and several other items are stored in the cookie by the SAP server, using standard public-key cryptographic routines. This design allows any SAP server to verify the user's identity without synchronizing passwords.

  This is particularly important in a SiteMinder environment since the username and password in the directory that SiteMinder uses do not match those of the SAP environment. You might also want to have single sign SAP-ITS on to other enterprise applications and resources.

Non-Password Authentication

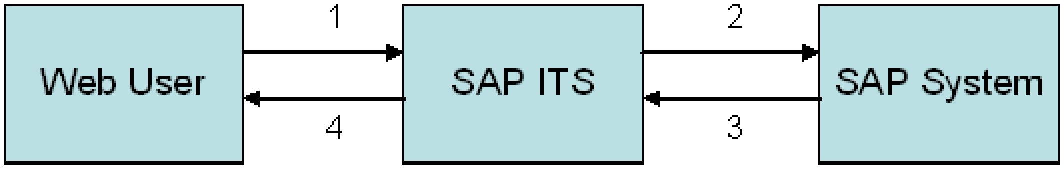
SiteMinder offers a multitude of authentication methods, many of which do not utilize a password at all; certificates is an example of non-password authentication.

SAP provides an API called Pluggable Authentication Service (PAS), which allows for authentication to occur through a process external to SAP. Once authenticated, SAP generates an SSO2 Ticket, allowing access by a user without a password to any SAP transaction.

Architecture

Standard SAP-ITS Environment

Without the SiteMinder Agent for SAP ITS integration, a typical SAP environment including ITS is shown in the following illustration:



This achieves SSO for SAP applications and resources, but does not allow for SSO beyond the SAP environment. The User logs in with a username and password and the SAP system returns content, along with the SSO Cookie or SSO Ticket, or both.

SAP-ITS and SiteMinder Environment

Once SiteMinder and the SiteMinder Agent for SAP ITS are integrated and enabled, the SiteMinder Web Agent operates normally, protecting the content on the web server running ITS. SiteMinder may be configured to protect individual SAP transactions. However, the recommended and more secure configuration is to protect all transactions. In the latter case, the policies would simply protect the virtual URL /scripts/wgate/ with any SiteMinder authentication scheme required. You may also create additional realms that use higher levels of authentication to protect individual transactions.

Once the user is authenticated and authorized by SiteMinder, the SiteMinder Web Agent allows ITS to carry on its normal processing of the request. A user who does not yet have an SAP SSO2 Ticket is be presented with an SAP login page. This page, in turn, calls the newly created ITS service *zsmsapsso,* which creates an SAP ticket and redirects the user to the appropriate transaction.

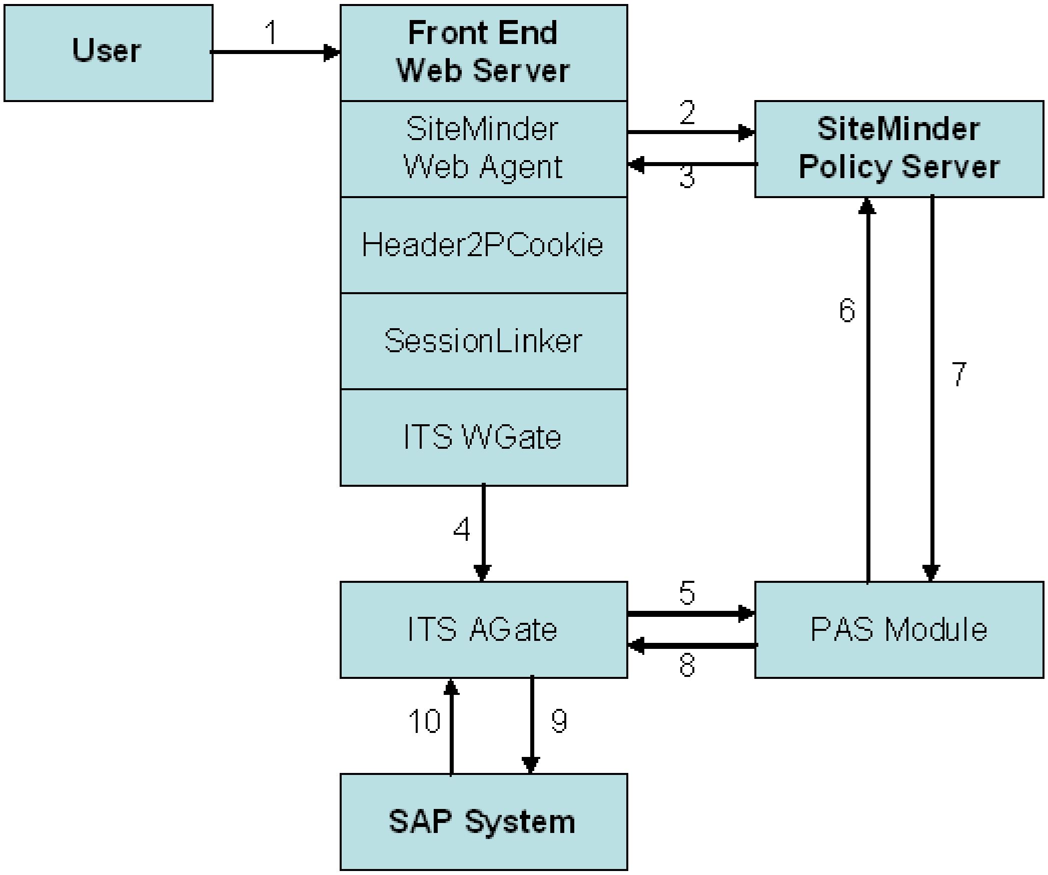
Note: The name of the *zsmsapsso* service is configurable.

Secured SAP-ITS and SiteMinder Environment

Two additional components are required to make the process secure; one enables secure pre-population of the SAP login page and the other maintains a one-to-one link between the SiteMinder and SAP sessions. Each is implemented as a web server add-on. These components are the following:

- Header to Pseudocookie (also called Header2PCookie), described in the *eTrust SiteMinder Agent - Header to Pseudocookie Guide*
- SessionLinker, described in the *eTrust SiteMinder Agent - SessionLinker Guide*.

The following illustration shows the data flow with the integrated SiteMinder Agent for SAP-ITS.



A description of the numbers in the preceding illustration follows:

1. User makes a request to the SAP application.
2. Web Agent checks SiteMinder Authentication and Authorization.
3. Result of Active response is passed to Web Agent, which in turn passes them as HTTP headers. The Header to Pseudocookie (Header2PCookie) component converts from HTTP headers to pseudocookies. A customized login page is then loaded and pre-populated with the contents of those pseudocookies. WGate processes the resulting page.
4. WGate passes the login request to AGate, which might or might not be on the same computer.
5. AGate calls the custom PAS module to verify username and SiteMinder session.
6. PAS module passes data to Policy server for verification.
7. Policy server returns the result to PAS module.
8. PAS module reports the result to AGate.
9. AGate requests an SAP SSO2 Logon Ticket from the SAP System.
10. SAP System returns SSO2 Ticket to AGate, which returns it to WGate, which in turns sends it back to the requesting system. Once an SSO2 ticket has been created, it is associated with the user's SiteMinder session and session divergence is prohibited via the Session Linker component.

Chapter 2: Installation

This section contains the following topics:

System Requirements

The following software is required:

- SiteMinder
  - SiteMinder Policy server 5.5 or later
  - SiteMinder Web Agent 5QMRx or later
- Front End Web Server
  - IIS 5 (or later),
  - SunOne Web Server 6.0 (or later) installed on Windows 2000
  - SessionLinker
  - Header To Pseudocookie (Header2PCookie)

- SAP
    - SAP Basis System 4.6D with 4.6D SAP Basis Support Package 03 or higher and a R/3 kernel patch level of at least 317
    - ITS 6.2
    - Workplace 2.11 (if workplace is installed)
    - ITS-Build 4640.3039.34.7423, Patch Level 39 or later must be installed on the ITS instance belonging to the Workplace Server
    - SNC between ITS (AGate) and R/3 server
    - sapextauth installed (or available) on the ITS AGate server.

Important! SiteMinder is not supported with the Integrated ITS for NW 2004. Since NW 2004 supports the stand-alone ITS 6.2, the SiteMinder Agent for SAP ITS can be used with the stand-alone ITS 6.2.

SiteMinder is not supported with the Integrated ITS for NW 2004s, while NW 2004s only supports the use of Integrated ITS. As a result, the SiteMinder Agent for SAP ITS cannot be used with NW 2004s.

Selecting a User Attribute

An attribute from the user directory to identify the user to SAP must be selected. When a user's entry in the directory contains the actual username used within SAP, no mapping is necessary. For example, the uid attribute in the LDAP directory might be the same as the SAP username. If this is the case, configure the Pluggable Authentication Service (PAS) service to use UN, which is the external ID. If the directory entry does not contain the SAP username, the mapping must be performed by SAP.

If SAP is to provide the mapping, the attribute used for mapping must be unique across the entire user population (it will likely be the user's Universal ID). An existing attribute, such as uid or the user's DN, could be used if the value is changed infrequently and cannot be modified by the end user.

Once the attribute has been selected, populate the SAP table USREXTID via the view VUSREXTID (transaction sm30) with the username to be returned by SiteMinder and the internal SAP username. SAP provides a number of external ID types for mapping. The only external ID type that applies in this case is ID, which you should use only if no other external authentication type is in use.

A patch will be available for R/3 that includes an additional mapping type SM. The external mapping type can be changed by modifying the ~extid_type setting in the zsmsapsso.srvc file.

The external ID is case sensitive. The content of the SiteMinder response must match the External ID field of USREXTID, including the case. The option ~login_to_upcase within the service file may be of assistance in this regard.

Installing the ERP Agent for SAP ITS

Installation is performed using the InstallAnywhere software developed by the Macrovision Corporation.

Installer can be run in the following modes:

- GUI mode for Windows or UNIX platforms
- Console mode for UNIX platforms

More information:

Run InstallAnywhere in GUI Mode (see page 16)

Run InstallAnywhere in Console Mode (see page 17)

Run InstallAnywhere in GUI Mode

Perform the following procedure in order to run InstallAnywhere in GUI mode.

To run InstallAnywhere in GUI mode

1. Access the executable file in the installation media, and click it. A window appears, with the caption InstallAnywhere is preparing to Install..., and a progress bar shows you the progress of the operation. When InstallAnywhere is loaded, the CA Siteminder ERP Agents v5.6 SP3 Introduction window appears.

   Note: It is recommended that you quit all programs before continuing with the installation.

2. Click Next. The License Agreement window appears. Read it.
3. Check the "I accept the terms of the License Agreement" check box, and click Next. The Important Information window appears.
4. Read the INSTALLATION NOTES and the DOCUMENTATION NOTES, and click Next. The Select an ERP Agent to Install window appears.
5. Check the radio button next to SAP ITS Agent, and click Next. The Finding Installed Software window appears.

   Elements of the SAP ITS agent must be installed on the following servers:

   - SAP ITS application server
   - SiteMinder web server, where the Web Agent has been installed.
   - SiteMinder Policy server

   Note: Depending on your configuration, whether the above-mentioned servers are located on the same or on different machines, you will need to run Installer once, twice or three times.

6. Mark the check box(es) next to the relevant software, and click Next. The Choose Install Folder window appears.
7. You must specify the location where you want the SAP ITS agent to be installed. A default folder C:\Program Files\CA\erpconn is indicated. You may accept the default folder or click Choose, browse to the required folder and click OK. Click Next. The Pre-Installation Summary window appears.
8. Review your selections, and click Previous to change any of your choices or click Install. The installation takes place, and a progress bar appears, indicating the installation of the Merge Module. When the installation is achieved, the Install Complete window appears: a message indicates that the installation is finished. In case errors occurred, a relevant message is issued. You are directed to view the installation log for details.

   Note: The log indicates the following:

   - Whether the installation succeeded or failed

- The number of successes
- The number on non-fatal errors
- The number of fatal errors

9. Click Done to exit InstallAnywhere.

Run InstallAnywhere in Console Mode

Perform the following procedure in order to run InstallAnywhere in console mode.

To run InstallAnywhere in console mode

1. Run the executable installer file from the command line, using the following command
   executable name -i console

   When InstallAnywhere is loaded, the CA Siteminder ERP Agents v5.6 SP3 Introduction window appears.

   Note: It is recommended that you quit all programs before continuing with the installation.

   Note: At any time during the installation procedure, you can enter Quit in order to exit the procedure.

2. Press Enter to continue. The License Agreement window appears. Read it, pressing Enter as necessary to view the whole text. At the end of the text, the "I accept the terms of the License Agreement" text appears.
3. Enter **Y** if you accept, and want to continue Installing the ERP Agent, and press Enter to continue. The Important Information window appears.

4. Read the INSTALLATION NOTES and the DOCUMENTATION NOTES, pressing Enter as many times as needed to reach the end of the text. The Select an ERP Agent to Install window appears. The options vary according to your platform. For example, on Windows, the options are as follows:

   1- SAP Web Application Server Agent

   2- PeopleSoft Agent

   3- Siebel Agent

   4- SAP ITS Agent

   You are prompted to ENTER THE NUMBER FOR YOUR CHOICE OR PRESS <ENTER> TO ACCEPT THE DEFAULT, which is marked by an arrow.

5. Enter the number that corresponds to SAP ITS Agent, and press Enter. The Finding Installed Software window appears.

   Elements of SAP ITS Agent must be installed on the following servers:

   1- SAP ITS application server

   2- Web server, where the Web Agent has been installed.

   3- Policy server

   Note: Depending on your configuration, whether the above-mentioned servers are located on the same or on different machines, you will need to run Installer once, twice or three times.

   You are prompted to ENTER A COMMA-SEPARATED LIST OF NUMBERS REPRESENTING THE DESIRED CHOICES OR PRESS <ENTER> TO ACCEPT THE DEFAULT, which is marked by an arrow.

6. Enter your selection, for example, 1,3, and press Enter. The Choose Install Folder appears.

7. You must specify the location where you want the SAP ITS agent to be installed. A default folder, *Path to your home directory*/CA/erpconn, is indicated. You may accept the default folder and press Enter or enter the full path to the required folder, and press Enter. The Pre-Installation Summary window appears.

8. Review your selections, and press Enter to Install. The installation takes place, and a progress bar appears. When the installation is complete, a confirmation message is issued. In case errors occurred, a relevant message is issued. You are directed to view the installation log for details.

   Note: The log indicates the following:

   - Whether the installation succeeded or failed
   - The number of successes
   - The number on non-fatal errors
   - The number of fatal errors

9. Press Enter to exit InstallAnywhere.

Installing Header to Pseudocookie

This component is necessary due to a limitation in the SAP B-HTML template processing. Pseudocookies appear to the underlying application as if they were presented by the user when, in fact, they were created by SiteMinder as responses from the Policy server. Security is enhanced and the user is prevented from replacing the content of the cookies in an attempt to bypass security.

When you install on the Web Agent/web server or on the Policy server, Header to Pseudocookie is installed by the InstallAnywhere installer as part of the installation of the Agent for SAP ITS.

For more information, see *eTrust SiteMinder Agent - Header to Pseudocookie Guide.*

Installing SessionLinker

The SessionLinker takes an application session cookie and associates it with a SiteMinder session cookie. Once associated, that application cookie (referred to, here, as the foreign session) can be used only by that particular SiteMinder session. SessionLinker prevents attempts by other SiteMinder sessions to use the same foreign session.

When you integrate applications that maintain their own sessions, one of the main security problems is the possibility that the SiteMinder and application sessions could become out of sync. The purpose of this component is to prevent such session synchronization issues. The SessionLinker monitors the SiteMinder Session ID header against the SAP SSO2 Ticket (MYSAPSSO2) and the ~session cookies. When these sessions diverge, action is taken to prevent the application from operating until a new session within SAP is established. By default, the action is to destroy the SSO2 Ticket and the ~session cookie. Once these cookies are removed, ITS is forced to create a new ticket and a new user session cookie with the correct user information included.

Installing SessionLinker occurs as part of the installation of the Agent for SAP ITS on the WEB Agent/web server or on the Policy server. See *eTrust SiteMinder Agent - SessionLinker Guide* for further details about SessionLinker*.*

Configuring SiteMinder Policies

Create a Test Realm and Policy

Perform the following procedure to create a test realm and policy.

To create a test realm and policy

1. Create a test realm for the resource /saptest/ on the web server hosting the WGate, by using any SiteMinder authentication scheme.
2. Create a rule protecting Get and Post within that realm.
3. Create a response that contains the following three Web Agent HTTP Header variables:
    - A User Attribute response. Set the following values:

      Variable Name set to SAPUSERNAME

      Attribute Name set to the attribute that should be presented to SAP.

      More information:

      Selecting a User Attribute (see page 15)
    - An Active Response for Header2PCookie. Set the following values:

      Variable Name should be blank

      Library Name set to npsheader2pcookie

      Function Name set to Config

      Parameter to SM_SERVERSESSIONID;SM_SERVERSESSIONSPEC; SAPUSERNAME (do not use spaces within the Parameter field).

      The attribute's value should be cached and

      Cache Value should remain selected.

      Click the Advanced tab and remove the first equal sign (the one preceding the less than sign). The results should appear as shown below:

```
<@lib="npsheader2pcookie" func="Config"
param="SM_SERVERSESSIONID;SM_SERVERSESSIONSPEC;SAPUSERNAME"@>
```

- An Active Response for SessionLinker. Set the following values:

  Variable Name should be blank

  Library Name set to npssessionlinker

  Function Name set to Config

  Parameters set to COOKIE1=MYSAPSSO2;COOKIE2=~session

  Click the Advanced tab and remove the leading equal sign (=). The result should appear as:

```
<@lib="npssessionlinker" func="Config"param="COOKIE1=MYSAPSSO2;COOKIE2=~session"@>
```

4. Create a Policy that includes rules and an appropriate set of users. Associate the responses with the rule created in Step 2.

Verify the SiteMinder Configuration

Perform the following procedure to verity the SiteMinder configuration.

To verify the SiteMinder configuration

1. On the web server, locate the following files that have been installed by Installer:

   SAP ITS agent installation folder/sapits/Configuration/inetpub/saptest.asp

   SAP ITS agent installation folder/sapits/Configuration/inetpub/saptest.exe

2. Through your web browser, try accessing the saptest.asp file. The resulting page indicates the configuration problems, if any.

In addition to displaying configuration details, the saptest.asp page also detects missed steps and provides suggestions for resolving problems.

Creating a Service Realm and Policy

Keep the test realm you created in Create a Test Realm and Policy (see page 20), and create a second realm to protect the service file:

/scripts/wgate/zsmsapsso

When you create this service realm, use the responses and policies that you used for the test realm.

SAP System Configuration Requirements

Overview

Before you install SiteMinder Agent for SAP ITS, the SAP and ITS environment must be in a known, working configuration. The following steps are necessary in the SAP environment:

- Enabling SAP Secure Network Connections (SNC) from the AGate to R/3
- Enabling the generation and acceptance of SSO2 Tickets

If necessary, configure the user mapping table (USREXTAUTH)

These steps are briefly described in the following sections.

For more information, see the SAP documentation.

Enable SNC Between AGate and R/3

Perform the following procedure to enable SNC between the ITS AGate and R/3.

To enable SNC between the ITS AGate and R/3

1. Open the ITS component's AGate global.srvc file. The following lines should appear within the file:

   ```
   ~sncNameR3 <Some value>
   ~sncQoPR3 <Some value>
   ```

2. Open the SAP front end and execute transaction rz11. Enter **snc/*** and click Display.
3. Set the following parameters:

   ```
   snc/enable 1
   snc/gssapi_lib <Some value>
   snc/data_protection/min 1
   snc/data_protection/max <Some value>
   snc/data_protection/use <Some value>
   snc/identity/as <Some value>
   ```

Other snc parameters may be present as well. For information on the correct settings for these parameters, see the SAP's SNC documentation.

Verify that SSO2 Tickets are Enabled

SSO2 Tickets are created by the R/3 server and, when received by ITS, can be used to sign onto an R/3 system. The generation of these tickets is a prerequisite for SiteMinder to SAP single signon.

To verify that the R/3 server is generating SSO2 tickets

1. Log in to the SAP front end and execute transaction SSO2.
2. Enter NONE in the text box and click Execute.
3. Examine the results. If every stoplight is green, the application server should be capable of issuing SSO2 Tickets.
4. Look for the following lines in the global.srvc file:

   ```
   ~cookies 1
   ~mysapcomusesso2cookie 1
   ```

   If SSO2 cookies are in use throughout your organization, add the following parameter for additional security:

   ```
   ~mysapcomnosso1cookie 1
   ```

5. Attempt to execute an ITS transaction such as webgui:

   (http://machine.domain.com/scripts/wgate/webgui/!)

   a. Enable cookie warnings.

      In Internet Explorer, select Tools, Internet Options, Security tab.

      In Netscape, select Edit, Preferences, Advanced.

   b. Enter your username and password, and click the Login button.

      Upon login, a warning message asks whether a cookie named MYSAPSSO2 can be saved to your computer. If this message (with this cookie name) appears, SSO2 Tickets are functioning properly.

Chapter 3: Configuration

This section contains the following topics:

Overview

Installation and configuration involves copying files installed by InstallAnywhere, and placing them on various servers. These files include the service file, templates, and SiteMinder files.

Installing and Configuring the Service File

Install the Service File

The service file, zsmsapsso.srvc is installed by Installer in the *SAP ITS agent installation folder*\sapits\configuration\services folder on the SAP ITS AGate server.

Copy it to the following location in the Program Files folder:

```
\SAP\ITS\6.20\<instance name>\services
```

Configure the Service File

To configure the service file, adjust the settings according to the description within the file. Refer to the following table for the settings specific to SiteMinder.

Setting	**Description**
~LogFile	(Optional) This is not a SiteMinder setting, however you may use it to specify a file name that the PAS module uses for logging. The PAS module does not log to the AGate trace file at this time.
~PolicyServer	IP address of Policy server used by Web Agent (see Specifying Multiple Policy Servers (see page 27)).
~PolicyServerFailover	(Optional) Specify YES or NO when specifying multiple Policy servers. The default is NO. As with Web Agent configuration, specifying YES means Policy servers are used in Failover; NO means requests are sent to each Policy server in the list in a round robin manner.
~AgentName	Agent name of the agent used to protect the service realm as mentioned in Create a Test Realm and Policy (see page 20); it should be enabled to support 4.x agents.
~SharedSecret	Shared Secret of the above-named Agent.
~Resource	The URI (*not URL*) of the zsmsapsso service. This should be a protected URI.

Specifying Multiple Policy Servers

If multiple Policy servers are to be used, enter all IP addresses on a single ~PolicyServer line, separated by a single space. By default, Policy servers are assumed to operate on the default ports 44441, 44442, and 44443 for Accounting, Authentication, and Authorization respectively. If Policy servers are operating on non-default ports, you must enter them in the following form:

```
IPAddress,AccountingPort,AuthenticationPort,AuthorizationPort
```

For example, if two Policy servers are in use, operating on ports 44441, 44442, and 44443 at IP addresses 192.168.1.4 and 192.168.1.5, the entry in the configuration file must be as shown below:

```
192.168.1.4,44441,44442,44443 192.168.1.5,44441,44442,44443
```

Note: The Accounting server is never used and the SAP Agent does not connect to the SiteMinder Accounting server under any circumstances. The Accounting port is entered here for consistency with the Web Agents and for future expansion.

Specifying SAP Settings

Additional settings in the file are specific to SAP.

For more information, see the SAP documentation.

Install the Templates

Perform the following procedure to install the templates.

To install the templates

1. Copy the zsmsapsso folder, located in the *SAP ITS agent installation folder*\sapits\config\templates folder to the templates folder of the SAP ITS installation folder.
2. Copy the login.html file located in the *SAP ITS agent installation folder*\sapits\config\templates\system\dm folder to the templates\system\dm folder of the SAP ITS installation folder.

Note: You may want to backup the existing login.html file before replacing it with the login.html file from the *SAP ITS agent installation folder*.

Install the PAS Module on Windows Platforms

The smsappas.dll and smagentapi.dll files are installed by Installer in the *SAP ITS agent installation folder*\sapits\bin folder on the SAP ITS AGate server.T

To install the PAS module

Copy the smsappas.dll and smagentapi.dll files into the following folder on the ITS AGate host: Program Files\SAP\ITS\6.20\Programs.

SiteMinder v5.x Web Agents use the Trusted Host model for authenticating themselves. The SiteMinder Agent for SAP ITS continues to use the Agent Name and Shared Secret model used in Version 4 and earlier Web Agents.

When you create an agent for the PAS module, make sure to add a check mark to the Support 4.x agent checkbox (located in the Agent dialog).

Note: This is the same as the agent used to protect the Service realm as mentioned in Verify the SiteMinder Configuration (see page 21) and the one mentioned in the zsmsapsso.srvc file.

Test the Installation and Configuration

When you have installed all of the components, test them is a matter of logging into SiteMinder and executing the ITS service zsmsapsso. For example, in a browser, open the following URL:

```
http://<location.of.wgate>/scripts/wgate/zsmsapsso/!
```

If successful:

- A screen appears. with the message: SAP session starting.

  Note: In some cases the entire screen might not appear before the next step is performed.

- The web browser acquires an SSO2 Ticket in a cookie and is redirected to the ITS transaction configured in the *SAP ITS agent installation folder*\sapits\config\services\zsmsapsso.srvc file. By default, this is the webgui, but it can easily be changed to the workplace or any other desired transaction by updating the service file.

If unsuccessful, see Troubleshooting and Messages (see page 29).

Chapter 4: Troubleshooting and Messages

This section contains the following topics:

Troubleshooting Installation and Configuration Problems

Symptom:

Installation or configuration did not succeed.

Solution:

Perform the following procedure to troubleshoot installation and configuration problems.

To troubleshoot installation and configuration problems

1. Check the SAP system configuration requirements. If any step has been missed or cannot be verified, customer support may not be able to assist.
2. Check Policies.

   Use the SiteMinder tool to verify the protection of /scripts/wgate/zsmsapsso for the user that you are attempting to use for testing. You should have the following responses:

   - NPS_SESSIONLINKER
   - NPS_HEADER2PCOOKIE
   - SAPUSERNAME

3. Verify the Web Agent function, as follows:

   a. Enable the Web Agent log, and restart the IIS or SunOne web server if necessary.

   b. Enable cookie warnings in your browser, and log in. Begin by accessing the saptest.asp page, as mentioned in Step 2 of Verifying the SiteMinder Configuration (see page 21). The SMSESSION cookie should be set. If it is not set, see the *eTrust SiteMinder Agent- Header to Pseudocookie Guide* for troubleshooting.

   c. Without closing your browser, access zsmsapsso. While the SAP session startup is in progress, several cookies should be set: one for the SAP session ID, one for the character set, and one for MYSAPSSO2. If the MYSAPSSO2 cookie is not set, the problem could be in either SAP or the service (zsmsapsso).

4. Temporarily disable SessionLinker.

   To simplify the environment, it may be worthwhile to temporarily remove the possibility of a problem in SessionLinker. Do not perform this step in production, as it may risk exposing the system to attacks.

5. Examine the zsmsapsso service log file.

   – If the operation was successful, the message Returning OK appears, meaning that the service is functioning properly and is receiving the appropriate content from the login.html page included in the zsmsapsso templates directory.

   – If the operation was unsuccessful, error conditions are logged, which are usually self-explanatory.

   More information:

   Messages in the Service Log File (see page 31)

6. Examine the ITS AGate and WGate trace files. If problem messages appear, see the SAP documentation for guidance.

7. Examine SAP traces. If problem messages appear, see the SAP documentation for guidance.

Messages in the Service Log File

Authentication Rejected

License EXPIRED or NOT VALID - authentication rejected

Symptom:

Authentication was rejected.

Solution:

Verify the validity of the license.

Agent Failed to Connect

Agent failed to connect

Symptom:

The message Agent failed to connect appears.

Solution:

The Agent name or shared secret might be incorrect. Check the Policy server logs for more information. In addition, verify the Policy server IP address or addresses.

Unable to Connect Agent

Unable to connect agent - missing a setting or 2

Symptom:

The message Unable to connect agent - missing a setting or 2 appears.

Solution:

One or more of the configuration settings for the agent are missing. It is likely that the configuration file in use is not correct because the default file provided includes defaults for these configuration settings.

Failed to Set Resource

Failed to Set Resource

Symptom:

The message Failed to set resource appears.

Solution:

The resource entered in the configuration file might not be protected by SiteMinder. See the Policy server's Authorization log for more information.

Session Validation Failed

Session validation FAILED

Symptom:

The message Session validation FAILED appears.

Solution:

The session ID, Spec and/or Username do not match or were not accepted by Policy server. Check the Policy server's Authentication and Authorization logs for more information. Additional error text may be displayed on the next line in the log file.

Access will be Denied

Access will be denied - License is not valid

Symptom:

The message Access will be denied - License is not valid appears.

Solution:

Check the validity of the license.

Agent not Ready to Validate

Agent not ready to validate

Symptom:

The message Agent not ready to validate appears.

Solution:

The possible cause of this error is that the license is not valid or the resource URI for the service realm is not protected. Check the validity of the license and the protection status of the resource URI.

Returning Denied

Returning denied

Symptom:

The message Returning denied appears.

Solution:

This generic error message is reached only when another error occurs. Examine the log file for that other error.

Appendix A: NPSEncrypt and NPSVersion Tools

This section contains the following topics:

NPSEncrypt Tool

Sometimes, *secret* values must be stored in a configuration file. For security purposes, you may want to encrypt and store the encrypted form of these secret values. To do this, use the NPSEncrypt tool. When a setting allows encrypted values to be used, this product will decrypt it before use. If the setting is not encrypted, the value entered will be used as is.

The NPSEncrypt utility takes plain text entered on the command line, encrypts it, and prints the result on the screen. The resulting encrypted text can be cut and pasted wherever it is needed.

A product that allows an encrypted value automatically decrypts the value when needed.

To encrypt a value, use the command prompt and type the NPSEncrypt command followed by a space and by the text to be encrypted:

```
C:\>npsencrypt secret
[NPSEncrypt Version 1.1 - NPSEncrypt Revision 1]
[NDSEnc-B]CKtyevyWkrF24Aj9Ly+xEQ==
```

In this case the encrypted form of secret is:

```
[NDSEnc-B]CKtyevyWkrF24Aj9Ly+xEQ==
```

When you copy and paste, grab the entire line, including [NDSEnc-B].

NPSEncrypt will encrypt the same text to many different cipher text values. Use any of the values, for example:

```
C:\>npsencrypt secret

[NPSEncrypt Version 1.1 - NPSEncrypt Revision 1]

[NDSEnc-C]iQO2KVyRN2fB4tMwjtgRYQ==

C:\>npsencrypt secret

[NPSEncrypt Version 1.1 - NPSEncrypt Revision 1]

[NDSEnc-C]FWhVC+MiA7aNnA87szw76g==

C:\>npsencrypt secret

[NPSEncrypt Version 1.1 - NPSEncrypt Revision 1]

[NDSEnc-B]PD24A2Iz6H+KeDh7j4zUIg==
```

NPSVersion Tool

Use the NPSVersion tool to extract version information from many CA products. To use this tool, type NPSVersion on a command line followed by a space and the name of the executable whose version information you want, for example:

```
C:\> NPSVersion sessionlinkd
[NPSVersion Version 1.0 - NPSVersion Revision 1]
sessionlinkd     -  Package: NPSSessionLinker V1.3
sessionlinkd     - Component: SessionLinker daemon V1.3.2 (Jul 14 2003 20:26:16)
sessionlinkd     -  Platform: AIX

C:\>
```

You may use the NPSVersion tool on one platform to extract information for a product built for any other platform. The actual information displayed might differ in format and content from that shown above, but the relevant lines when discussing any issues with Support are Package and Component. Each line has a version number.

Package refers to the version of the Product, in this case the SessionLinker version 1.3 product.

Component refers to the actual part of the product that is enclosed within this specific file. It is not uncommon for this version number to be larger than the *Package* version. This is usually due to the Component having one of more defects repaired or minor enhancements added that did not require the entire Package to be rebuilt or renumbered.

Index